REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed April 16, 2007. Claims 1-17 remain pending in the present application. Reconsideration and allowance of the application and pending claims are respectfully requested.

1. Response to Rejections of Claims under 35 U.S.C. §112

Claim 9 has been rejected under 35 U.S.C. § 112, Second Paragraph, as allegedly being indefinite. In particular, claim 9 is alleged to have insufficient antecedent basis for the phrase "the network enquiry." In response, claim 9 has been amended to provide further clarification and is believed to overcome the rejection. Therefore, withdrawal of the rejection is respectfully requested.

2. Response to Rejections of Claims under 35 U.S.C. §102

Claims 1-17 have been rejected under 35 U.S.C. §102(e) as being anticipated by *Herzi* (U.S. Patent No. 6,484,262). Applicant respectfully traverses this rejection.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed subject matter must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. §102(e). In the present case, not every feature of the claimed subject matter is represented in the *Herzi* reference.

a. Claim 1

As provided in independent claim 1, Applicant claims:

> A component for a computer, the component comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and

permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,

the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check.

(Emphasis added).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that *Herzi* does not disclose, teach, or suggest at least "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited and emphasized above in claim 1.

Rather, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose that a "security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 1. Further, *Herzi* does not describe the security check of claim 1 in the manner claimed.

For at least these reasons, *Herzi* does not teach or suggest all of the features of claim 1, and the rejection of claim 1 should be withdrawn.

b. Claims 2-9

Because independent claim 1 is allowable over the cited art of record, dependent claims 2-9 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that dependent claims 2-9 contain all the

features of independent claim 1. For at least this reason, the rejections of claims 2-9 should be withdrawn.

c. Claim 10

As provided in independent claim 10, Applicant claims:

> A component for a computer, the component comprising a firmware element operable to:
>
> generate a random number to be used in performing a security check to verify the computer is connected to an authorised network,
>
> encrypt the random number with a public key of a public/private key pair associated with an authorised network,
>
> transmit the encrypted random number to a network device via the network,
>
> receive a response comprising a number from the network device,
>
> compare the random number transmitted to the network device with the number in the response, and
>
> ***permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check.***

(Emphasis added).

Applicant respectfully submits that independent claim 10 is allowable for at least the reason that *Herzi* does not disclose, teach, or suggest at least "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited and emphasized above in claim 10.

Rather, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 10. Further, *Herzi* does not describe the security check of claim 10 in the manner claimed.

For at least these reasons, *Herzi* does not teach or suggest all of the features of claim 10, and the rejection of claim 10 should be withdrawn.

d. Claim 11

As provided in independent claim 11, Applicant claims:

> A BIOS for a computer, the BIOS being operable to perform a security check to verify the computer is connected to an authorised network as part of a boot process, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and
>
> comparing the random number transmitted to the network device with the number in the response; and
>
> ***preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check***.

(Emphasis added).

Applicant respectfully submits that independent claim 11 is allowable for at least the reason that *Herzi* does not disclose, teach, or suggest at least "preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited and emphasized above in claim 11.

Rather, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose "preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous

security check," as recited in claim 11. Further, *Herzi* does not describe the security check of claim 11 in the manner claimed.

For at least these reasons, *Herzi* does not teach or suggest all of the features of claim 11, and the rejection of claim 11 should be withdrawn.

e. Claim 12

As provided in independent claim 12, Applicant claims:

> A computer comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and
>
> permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,
>
> ***the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check***.

(Emphasis added).

Applicant respectfully submits that independent claim 14 is allowable for at least the reason that *Herzi* does not disclose, teach, or suggest at least "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited and emphasized above in claim 12.

Rather, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration

of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 12. Further, *Herzi* does not describe the security check of claim 12 in the manner claimed.

For at least these reasons, *Herzi* does not teach or suggest all of the features of claim 12, and the rejection of claim 12 should be withdrawn.

f. Claims 13-16

Because independent claim 12 is allowable over the cited art of record, dependent claims 13-16 (which depend from independent claim 12) are allowable as a matter of law for at least the reason that dependent claims 13-16 contain all the features of independent claim 12. For at least this reason, the rejections of claims 13-16 should be withdrawn.

g. Claim 17

As provided in independent claim 17, Applicant claims:

> In combination, a computer comprising an element operable to perform a security check to verify the computer is connected to an authorised network and a network device operable to receive a network enquiry from the computer over a network, the element being operable to:
>
> generate a random number,
>
> encrypt the random number with a public key of a public/private key pair associated with the network, and
>
> transmit the encrypted random number to the network device via the network,
>
> the network device being operable to:
>
> receive the encrypted random number from the computer,
>
> decrypt the encrypted random number using the private key of the public-private key pair, and
>
> generate a response comprising the random number and transmit the response to the computer;
>
> the element being operable to:
>
> receive the response comprising from the network device,

compare the random number transmitted to the network device with the number in the response, and

permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.

(Emphasis added).

Applicant respectfully submits that independent claim 17 is allowable for at least the reason that *Herzi* does not disclose, teach, or suggest at least "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited and emphasized above in claim 17.

Rather, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 17. Further, *Herzi* does not describe the security check of claim 17 in the manner claimed.

For at least these reasons, *Herzi* does not teach or suggest all of the features of claim 17, and the rejection of claim 17 should be withdrawn.

CONCLUSION

For at least the reasons set forth above, Applicant respectfully submits that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

Respectfully submitted,

Charles W. Griggers, Reg. No. 47,283